UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/660,476	09/12/2003	Hee-Kwan Son	2557-000181/US	6312

30593 7590 05/09/2008

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 8910
RESTON, VA 20195

EXAMINER	
YAARY, MICHAEL D	

ART UNIT	PAPER NUMBER
2193	

MAIL DATE	DELIVERY MODE
05/09/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Supplemental Notice of Allowability	**Application No.** 10/660,476	**Applicant(s)** SON, HEE-KWAN	
	Examiner MICHAEL YAARY	**Art Unit** 2193	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☐ This communication is responsive to _____.

2. ☒ The allowed claim(s) is/are *1-15, 17, 18, 21 and 22*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

/Lewis A. Bullock, Jr./
SPE, AU 2193

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Larry Galvin on 03/14/2008.

This is to correct the status of the claims from the previous notice of allowance mailed 04/07/2008, and these are the same changes sent then.

The claims have been amended as follows:

2. In claim 1, replace line 19 with, "an S-register in which a bit value s_i of the sum S is updated and stored; and"

3. In claim 1, replace line 20 with, "a C-register in which a bit value c_i of the carry C is updated and stored."

4. In claim 18, replace line 16 with "an S-register in which a bit value s_i of the sum S is updated and stored; and"

5. In claim 18, replace line 17 with “a C-register in which a bit value c_i of the carry C is updated and stored;”

6. In claim 18, replace lines 1-2 with, “A system embodying a Montgomery modular multiplier of a public-key cryptographic system, the system comprising:

7. Claims 19-20 cancelled.

8. In claim 21, line 2, replace -a public key- with "the public-key"

REASONS FOR ALLOWANCE

9. Claims 1-15, 17, 18, 21, and 22 are allowed.

10. The following is an examiner’s statement of reasons for allowance:

11. The prior art of record fails to teach or suggest the claimed invention. Specifically the prior art of record fails to teach or suggest the Montgomery modular multiplier structure having at least a q_i calculation logic circuit solving a Boolean logic equation “s_0 XOR c_0 XOR (b_i AND a_0),” and a compressor performing n additions on the carry C, the

sum S, the b_iA, and the q_iM to obtain interim values and summing the interim values to obtain a result using a carry propagation adder in response to a carry propagation adder signal, as recited in independent claims 1, 7, 17, and 18.

12. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL YAARY whose telephone number is (571)270-1249. The examiner can normally be reached on Monday-Friday, 8:00 a.m - 5:00 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Lewis Bullock can be reached on (571) 272-3759. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. Y./
Examiner, Art Unit 2193

/Lewis A. Bullock, Jr./

Supervisory Patent Examiner, Art Unit 2193